IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF THE DEVICES LISTED ON ATTACHMENT A, CURRENTLY LOCATED AT 100 EDISON PARK DRIVE, GAITHERSBURG, MARYLAND, 20878

Case No. 17-3095-CBD

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

INTRODUCTION AND AGENT BACKGROUND

1. I, James Walsh, Task Force Officer (TFO) of the Federal Bureau of Investigation (FBI), Baltimore Division (BA), Rockville, Maryland, being duly sworn, depose and state as follows:

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

3. Your affiant is a Detective with Montgomery County Police Department (MCPD), Special Investigations Division, Drug Enforcement Section, Major Offenders/Conspiracy Unit and has been so employed with Montgomery County Police since July 2008. Prior to being employed with Montgomery County Police, from October 2001 to July 2008, your affiant was a sworn law enforcement officer with the United States Park Police. Your affiant has been specially deputized as a Task Force Officer (TFO) by the Federal Bureau of Investigation (FBI) since October of 2014. Your affiant graduated from the Federal Law Enforcement Training Center (FLETC) in 2002 and the MCPD Training Academy in January

SW
CBD

2009. In sixteen years as a law enforcement officer your affiant has investigated a myriad of criminal offenses to include wire fraud and narcotic offenses.

4. During my sixteen years as a law enforcement officer, to include the past four years of conducting undercover narcotics investigations, your affiant has performed controlled purchases of drugs and street level surveillance of drug transactions; utilized informants to make controlled purchases of drugs; worked in an undercover capacity on several occasions involving narcotics investigations targeting street level and interstate narcotics traffickers; obtained and executed search warrants as a result of drug investigations; attended numerous courses and seminars covering drug recognition, interdiction, money laundering, conspiracy investigations and secure communications interception; participated in and been a co-case agent on Title III wiretap investigations involving federal narcotics violations; and been recognized as an expert in narcotics trafficking by the Circuit Court and Juvenile Court for Montgomery County, Maryland.

5. Your affiant has been involved in the investigation of several Organized Crime Drug Enforcement Task Force (OCDETF) investigations involving drug trafficking organizations. Your affiant has extensive experience in debriefing defendants, working with confidential informants, and various persons with direct experience with the methods used to distribute controlled substances.

6. Your affiant has also attended numerous other training classes and seminars related to undercover narcotics investigations, drug interdiction, conducting interviews, drug recognition and fraud and money laundering. Additionally, your affiant has developed, taught and continues to teach several continuing educational courses to sworn officers on drug investigations

SW
CBD

7. Based on your affiant's training and experience, your affiant is familiar with the means and methods that narcotics traffickers use to import and distribute illicit drugs. Your affiant is familiar with the means and methods individuals and groups of individuals use to commit various types of credit card fraud and identity theft. Your affiant is familiar with the support and assistance that narcotics organizations require to conduct their illegal activities. Your affiant has also become knowledgeable about the criminal statutes of the United States, particularly in the laws relating to violations of the federal narcotics, conspiracy, and fraud statutes.

8. Through this training and experience, your affiant has learned about the importation, manufacture, concealment and distribution of controlled substances, including, for example, cocaine, heroin, phencyclidine (PCP), and marijuana. Your affiant has become familiar with the use of telephones by drug traffickers to communicate, the patterns of activity of drug traffickers, the types and amounts of profits made by drug dealers, and the methods, language, and terms that are used to disguise the source and nature of the profits of illegal drug dealing. Additionally, based on your affiant's training and experience and his participation in other narcotics investigations, your affiant knows the following: that it is common for drug dealers to "front," or provide on consignment, controlled substances to their customers; that it is common for drug dealers to conceal contraband, proceeds of drug sales, and records of drug transactions in secure locations within their residences, vehicles and/or businesses for ready access; that it is common for drug dealers to conceal proceeds from law enforcement authorities and rival narcotics traffickers; that drug dealers routinely use cellular telephones to facilitate their drug distribution operations; that drug dealing is an ongoing process that requires the development, use, and protection of a communication network to facilitate daily drug

JW
CBD

distribution; that drug dealers use telephones to thwart law enforcement efforts to penetrate the drug dealers' communication networks; and that narcotics traffickers commonly use "coded" language when speaking with other drug traffickers in order to thwart detection by law enforcement agents who may be intercepting their communications.

9. Based upon my training and experience and my participation in this and other narcotics investigations, as well as my conversations with other agents, I know the following:

a. Narcotics traffickers often maintain at locations including their residences, businesses, vehicles, and stash houses, financial records and financial instruments related to their narcotics transactions and the profits derived from those transactions including, but not limited to, currency, bank checks, cashier's checks, Western Union receipts, money orders, stocks, bonds, precious metals, and real estate records;

b. Narcotics traffickers frequently maintain at locations including their residences, businesses, vehicles, and stash houses, records of their narcotics transactions including, but not limited to, books, ledgers, records and other documents relating to the manufacture, transportation, possession, and distribution of controlled substances. Such documents are frequently maintained where the traffickers have ready access to them, including in their homes;

c. Narcotics traffickers commonly maintain at locations including their residences, businesses, vehicles, and stash houses, identification and travel documents, including, but not limited to, tickets, transportation schedules, passports, notes and receipts related to travel, and motel/hotel receipts;

f. Indicia of occupancy, residency and/or ownership of the premises to be searched are often present in such premises;

g. Narcotics traffickers commonly maintain many of the foregoing items in cellular telephones, computer files, on disks, and on hard drives; removable storage devices such as "Thumb Drives" and

h. Narcotics traffickers commonly maintain at locations including their residences, businesses, vehicles, and stash houses, numerous cellphones that they use to contact their coconspirators, including their sources of supply, their distributors, and their customers.

10. Your Affiant knows that individuals involved in drug trafficking often use video recording devices, including cellular telephones, to take video recordings of other members of their organization often engaging in illegal activities such as the distribution of narcotics, as well as video recordings documenting the purchase of assets with the proceeds of narcotics trafficking.

11. Your Affiant knows that individuals involved in the fraudulent altering of others' credit card information for the purpose of obtaining merchandise while having the card holder billed for the purchases must procure personal identity information ("PII"), including a card holder's name, associated with the card holder accounts. This PII may be stored either electronically or in hard copy. The PII is often obtained from third party sources, and individuals involved in the conspiracy will use electronic devices, such as computers and cellular telephones, to communicate with co-conspirators. Further, individuals involved in such fraud will frequently use cellular telephones and other electronic devices to communicate with the credit card companies (to alter the information) and retail stores where the items were fraudulently purchased.

JW
CBD

12. Your Affiant knows that individuals involved in the fraudulent altering of others' credit card information for the purpose of obtaining merchandise while having the card holder billed for the purchases must use a wire to make the online fraudulent purchase via credit card.

13. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

14. The property to be searched are:

(a) Galaxy S7 cellular phone IMEI 357425074173145 (**TARGET DEVICE #1**) seized from George ABANKWA's person;

(b) Apple iPhone 5 cellular phone Serial #F76SFGJEHG71 seized Robert DARKO's person (**TARGET DEVICE #2**);

(c) LG cellular phone Serial #007CYVU0089039 seized from the trunk of DARKO's Honda sedan (**TARGET DEVICE #3**);

(d) Samsung cellular phone Serial #R21CA41ASRW seized from the trunk of DARKO's Honda sedan (**TARGET DEVICE #4**);

(e) Blackberry cellular phone Serial #356552045007945 seized from the trunk of DARKO's Honda sedan **(TARGET DEVICE #5**);

(f) Motorola cellular phone IMEI#359298050818027 seized from the residence at 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #6**);

(g) Kyocera cell phone FCC#V6553015, seized from the residence at 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #7**);

CBD

(h) Samsung cell phone FCC#A3LSMB311V, seized from the residence at 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #8**);

(i) Apple iPhone cell phone IMEI#03991007, seized from the residence at 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #9**);

(j) Samsung cell phone, dark in color, no identifying marks, MCPD evidence barcode 06143087, seized from the residence at 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #10**);

(k) Samsung cell phone, dark in color, no identifying marks, MCPD evidence barcode 06143072, seized from 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #11**);

(l) Samsung cell phone, dark in color, no identifying marks, MCPD evidence barcode 06143071, seized from 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #12**);

(m) Apple I-Phone cell phone with black case, MCPD evidence barcode 06143070, seized from 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #13**)

(n) Samsung S6 blue cell phone, no identifying marks, MCPD evidence barcode 06143093, seized from 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #14**)

(collectively referred to as the "**TARGET DEVICES**"). The **TARGET DEVICES** are currently located at the secure headquarters of the Montgomery County Police Department in Gaithersburg, Maryland, located at 100 Edison Park Drive, Gaithersburg, Maryland 20878.

15. The applied-for warrant would authorize the forensic examination of the **TARGET DEVICES** for the purpose of identifying electronically stored data particularly described in **Attachment B**.

PROBABLE CAUSE

16. Your affiant submits that there is probable cause to believe that there is evidence located in the **TARGET DEVICES** concerning the following offenses: (1) conspiracy to possess with intent to distribute and to distribute a controlled substance, in violation of 21 U.S.C. § 846; and (2) possession with intent to distribute and to distribute a controlled substance, in violation of 21 U.S.C. § 841; (3) wire fraud, in violation of 18 U.S.C. § 1343; and (4) aggravated identity theft, in violation of 18 U.S.C. § 1028A.

The Investigation

17. On June 28, 2017, Montgomery County Police Department (MCPD) law enforcement officers were conducting an investigation involving credit card fraud and theft of merchandise through online purchasing. It was discovered through contact with Corporate Asset Protection investigators of a large commercial retail chain and fraud investigators of Chase Bank that several of their customers had recently had their account address changed without the customer's knowledge or consent. The addresses were changed to "19111 Sweet Shrub Circle, Clarksburg, Maryland." None of the customers reported having any connection to this address; additionally these customers reported that several thousand dollars in merchandise was fraudulently purchased with their credit cards. The purchaser of these fraudulently purchased items had requested that they be delivered to 19111 Sweet Shrub Circle, Clarksburg, Maryland.

18. On June 26, 2017, law enforcement learned that items purchased using compromised credit cards were scheduled to be delivered at 19111 Sweet Shrub Circle, Clarksburg, Maryland on June 28, 2017. As a result, law enforcement conducted surveillance on the residence. Just after the fraudulently purchased packages were delivered, an individual later identified as George ABANKWA arrived at 19111 Sweet Shrub Circle in Clarksburg,.

JW
CBD

ABANKWA entered the residence and within minutes was seen loading packages into his vehicle. ABANKWA then departed in the same vehicle, until he was stopped and placed under arrest for numerous theft and credit card offenses under the Maryland state law. At the time of his arrest, ABANKWA was in possession of several packages that were the subject of the original fraudulent purchases tracked by law enforcement. Pursuant to ABANKWA's arrest, a Galaxy Samsung S7 cell phone was seized from his person (**TARGET DEVICE #1**).

19. Law enforcement confirmed that ABANKWA was the leaseholder of a residential apartment located at 12402 Great Park Circle, Apartment 104, in Germantown, Maryland. Chase Bank fraud investigators advised law enforcement that several different packages of fraudulently purchased merchandise were scheduled to be delivered to this residence. Like the fraudulent purchases of merchandise sent to 19111 Sweet Shrub Circle, Clarksburg, Maryland, these packages were also purchased promptly after an address change request was processed, for an existing Chase credit account, changing the existing account address to 12402 Great Park Circle, Apartment 104, Germantown, Maryland.

20. On June 28, 2017, law enforcement officers were conducting surveillance at 12402 Great Park Circle, Apartment 104, Germantown, MD while obtaining a search warrant for the same. During this surveillance, a black male, later identified as Robert DARKO, was observed entering Apartment 104. A short time later DARKO was observed exiting the residence carrying a small black Gucci bag, entering a dark Honda sedan and then driving out of the apartment complex parking lot. Prior to leaving in the Honda sedan, DARKO placed the black Gucci bag he was carrying in the trunk of the Honda. MCPD law enforcement officers subsequently observed the Honda sedan commit three moving violations and conducted a traffic stop. DARKO, the lone occupant, consented to a search of the Honda sedan.

21. The Honda sedan was then searched by MCPD law enforcement officers. Law enforcement discovered in the trunk of the Honda the black Gucci bag referenced above. Inside the black bag were two large plastic bags, each containing a chunky brown powder substance. The substance was later field-tested returning positive for heroin. The amount of heroin recovered weighed approximately 400 grams. DARKO was placed under arrest. An Apple iPhone cellular phone (**TARGET DEVICE #2**) was seized from DARKO's person at the time of his arrest. Seized from inside the black Gucci bag were three other cell phones, an LG cellular phone (**TARGET DEVICE #3**), a Samsung cellular phone (**TARGET DEVICE #4**), and a Blackberry cellular phone (**TARGET DEVICE #5**).

22. On June 28, 2017 MCPD law enforcement officers executed a Montgomery County Circuit Search and Seizure warrant at 12402 Great Park Circle, Apartment 104, Germantown, Maryland. Apartment 104 contained two bedrooms, one identified by its contents, including personal documents, as belonging to DARKO, the other ABANKWA. Both ABANKWA and DARKO were in custody at the time of the execution of the search warrant, and there was no indication of any other individual residing there aside from DARKO and ABANKWA. The following items were seized:

(a) Miscellaneous documents in the name of Robert DARKO and George ABANKWA;

(b) Motorola cellular phone IMEI#359298050818027 (**TARGET DEVICE #6**);

(c) Kyocera cellular phone FCC#V6553015 (**TARGET DEVICE #7**)

(d) A black digital scale;

(e) Numerous shoes, purses, bags and clothing accessories new in boxes;

(f) 12 tightly packed plastic capsules containing an unknown substance. It should be noted that the unknown substance later field tested positive for heroin. The total weight of these capsules was approximately 130 grams;

(g) Samsung cellular phone FCC#A3LSMB311V (**TARGET DEVICE #8**);

(h) Apple I-Phone cellular phone IMEI#03991007 (**TARGET DEVICE #9**);

(i) Newly purchased sneakers and sandals;

(j) Lenova Laptop Serial# P200DZKK ;

(k) Toshiba Laptop Serial#99457085K ;

(l) Toshiba Laptop Serial#XB21653Q ;

(m) Samsung cell phone, dark in color, no identifying marks (MCPD evidence barcode 06143087) (**TARGET DEVICE #10**);

(n) Samsung cell phone, dark in color, no identifying marks (MCPD evidence barcode 06143072) (**TARGET DEVICE #11**);

(o) Samsung cell phone, dark in color, no identifying marks (MCPD evidence barcode 06143071) (**TARGET DEVICE #12**);

(p) Apple I-Phone cell phone with black case (MCPD evidence barcode 06143070) (**TARGET DEVICE #13**);

(q) Samsung S6 blue cell phone, no identifying marks (MCPD evidence barcode 06143093) (**TARGET DEVICE #14**);

(r) Dell Laptop Serial# 7VX9042.

Item (f) was submitted to the MCPD crime lab for analysis, where it was determined to include 130.79 grams of heroin.

23. On June 30, 2017, law enforcement obtained the recorded jail calls of ABANKWA while he was in custody at the Montgomery County Central Processing Unit on June 28, 2017. Portions of these calls were in English while other portions were in an African dialect, Twi. As such, law enforcement had these calls translated by a qualified FBI Twi contract linguist. The calls revealed that after he was arrested on June 28, 2017, ABANKWA

made a phone call at 7:35 p.m. to a female who law enforcement believe is a woman identified as Individual C. Individual C is a personal associate of ABANKWA who resides at the original address where the fraudulently purchased packages were delivered and ABANKWA was first observed, 19111 Sweet Shrub Circle, Clarksburg, MD. During that call, ABANKWA asked Individual C to drive to his residence at 12402 Great Park Circle Apartment 104, and attempt to make contact with his roommate, DARKO. Individual C complied and arrived at the residence. Individual C was heard on the recorded call walking and then could be heard handing the telephone off to a male, whom law enforcement recognized to be DARKO.

24. Law enforcement officers were conducting physical surveillance while procuring a search warrant for 12402 Great Park Circle, Apartment 104 at 7:35 p.m. on June 28, 2017. This surveillance was ongoing at the time of ABANKWA's call to Individual C. As described above, at the same time that the recorded jail call from ABANKWA to Individual C was ongoing, officers observed a female arrive to the apartment building, and walk toward Apartment 104, talking on the telephone in the apartment breezeway. Individual C then entered the residence.

25. On this same call, after Individual C handed the telephone to DARKO, ABANKWA advised DARKO that ABANKWA had been arrested. ABANKWA asked DARKO if he remembered the "stuff" DARKO had been hiding for ABANKWA. Based upon your affiant's training and experience in this investigation and others, when ABANKWA referred to "stuff" it was coded language for illicit drugs. DARKO acknowledged the "stuff." ABANKWA provided DARKO two different ways to destroy the drugs. First, ABANKWA instructed DARKO to drop the drugs in the toilet and discard the remaining drugs through the bathtub by allowing them to soak, burst, and then eventually wash away. ABANKWA also

instructed DARKO to depart the residence with all the cellular phones. ABANKWA encouraged DARKO to do this quickly and vacate the residence. Within approximately 18 minutes after the phone call ended, law enforcement conducting the above-described surveillance of 12402 Great Park Circle Apartment 104 observed DARKO exit the residence and depart in the Honda sedan.

26. The **TARGET DEVICES** were submitted to the MCPD Evidence Unit for storage, where they have remained.

TECHNICAL TERMS

27. Based on your Affiant's training and experience, the term "wireless telephone" (or mobile telephone, or cellular telephone) refers to a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

ANALYSIS

28. Based on knowledge, training, and experience, you Affiant knows that the electronic **TARGET DEVICES** can store information for long periods of time. Similarly,

things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. There is probable cause to believe that things that were once stored on the **TARGET DEVICES** may still be stored there, for at least the following reasons:

a. Based on his knowledge, training, and experience, your Affiant knows that digital files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium such as a wireless telephone, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

30. *Forensic evidence.* As further described in **Attachment B**, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **TARGET DEVICES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices, or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **TARGET DEVICES** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

32. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

33. Your Affiant submits that this affidavit supports probable cause for a search warrant authorizing the examination of the **TARGET DEVICES** described in **Attachment A** to seek the items described in **Attachment B**.

Respectfully submitted,

James Walsh, Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me
on November 16, 2017:

Hon. Charles B. Day
United States Magistrate Judge

ATTACHMENT A

The property to be searched is listed below and is referred to collectively as the "TARGET DEVICES". The TARGET DEVICES are currently located at 100 Edison Park Drive, Gaithersburg, Maryland, 20878.

(a) Galaxy S7 cellular phone IMEI 357425074173145 (**TARGET DEVICE #1**) seized from George ABANKWA's person;

(b) Apple iPhone 5 cellular phone Serial #F76SFGJEHG71 seized Robert DARKO's person (**TARGET DEVICE #2**);

(c) LG cellular phone Serial #007CYVU0089039 seized from the trunk of DARKO's Honda sedan (**TARGET DEVICE #3**);

(d) Samsung cellular phone Serial #R21CA41ASRW seized from the trunk of DARKO's Honda sedan (**TARGET DEVICE #4**);

(e) Blackberry cellular phone Serial #356552045007945 seized from the trunk of DARKO's Honda sedan **(TARGET DEVICE #5**);

(f) Motorola cellular phone IMEI#359298050818027 seized from the residence at 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #6**);

(g) Kyocera cell phone FCC#V6553015, seized from the residence at 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #7**);

(h) Samsung cell phone FCC#A3LSMB311V, seized from the residence at 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #8**);

(i) Apple iPhone cell phone IMEI#03991007, seized from the residence at 12402 Great Park Circle, Apartment 104, Germantown, Maryland (**TARGET DEVICE #9**).

(j) Samsung cell phone, dark in color, no identifying marks (MCPD evidence barcode 06143087) (**TARGET DEVICE #10**);

(k) Samsung cell phone, dark in color, no identifying marks (MCPD evidence barcode 06143072) (**TARGET DEVICE #11**);

(l) Samsung cell phone, dark in color, no identifying marks (MCPD evidence barcode 06143071) (**TARGET DEVICE #12**);

(m) Apple I-Phone cell phone with black case (MCPD evidence barcode 06143070) (**TARGET DEVICE #13**);

(n) Samsung S6 blue cell phone, no identifying marks (MCPD evidence barcode 06143093) (**TARGET DEVICE #14**).

This warrant authorizes the forensic examination of the TARGET DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the TARGET DEVICES described in Attachment A that relate to violations of 21 U.S.C. § 846, 21 U.S.C § 841, 18 U.S.C. § 1343, and 18 U.S.C. § 1028A, and involve the defendants, George ABANKWA and Robert DARKO, and other coconspirators, including but not limited to:

a. lists of customers and related identifying information; data that may identify the owner or user of the TARGET DEVICES;

b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

c. types, amounts, and prices of merchandise obtained by credit card activity, as well as dates, places, and amounts of specific transactions;

d. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

e. any information related to sources of the personal identifying information ("PII") used to change the addresses of credit account holders prior to making fraudulent purchases on the account holders' card;

f. any information recording any of ABANKWA and DARKO's schedules or travels;

g. all bank records, checks, credit card bills, account information, and other financial records;

h. e-mails, text messages, and other communications and notes regarding ABANKWA and DARKO's and their coconspirators' narcotics trafficking and/or

fraudulent credit transaction activities, as well as audio and video clips related to said activities;

i. Global position system (GPS[1]) data including, but not limited to coordinates, way points and tracks;

j. Documents and other text based files related to narcotics trafficking and fraudulent use of credit cards.

2. Evidence of user attribution showing who used or owned the TARGET DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records of Internet Protocol addresses used;

4. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

---

[1] The Global Positioning System (GPS) is a satellite-based navigation system which provides location and time information.